UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,408	12/28/2000	Nicholas Sauriol	56130.000067	5257

7590 08/27/2008

James G. Gatto, Esq.
Hunton & Williams
Suite 1200
1900 K Street, N.W.
Washington, DC 20006

EXAMINER	
ELISCA, PIERRE E	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
08/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte NICHOLAS SAURIOL and ALEX SAURIOL

Appeal 2008-3749
Application 09/749,408
Technology Center 3600

Decided: August 27, 2008

Before MURRIEL E. CRAWFORD, HUBERT C. LORIN, and MICHAEL W. O'NEILL, *Administrative Patent Judges*.

LORIN, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Nicholas Sauriol, et al. (Appellants) seek our review under 35 U.S.C. § 134 of the final rejection of claims 1-12. We have jurisdiction under 35 U.S.C. § 6(b) (2002).

SUMMARY OF DECISION

We AFFIRM. [1]

THE INVENTION

"The present invention relates generally to electronic commerce (E-commerce), or commerce conducted over an interconnected processor based network and, more particularly, to a technique for providing a secured network which maintains consumer financial information in a secure fashion to enable users to make E-commerce transactions." (Specification 1:4-10). "One drawback of existing E-commerce systems is that when a consumer makes a purchase on-line (i.e., over the network, or on the Internet), most often it is over an unsecured line. As its name suggests, an unsecured line is susceptible to tampering, interception and other fraudulent activities." (Specification 2:1-6). "[I]t would be desirable to provide a technique for providing a database which maintains customer financial information in a secure fashion to enable customers and merchants (collectively, "users") to make E-commerce transactions in an efficient and cost effective manner." (Specification 3:20-4:3). "According to the present invention, a technique for providing a system and method that enables vendors and consumers to conduct E-commerce transaction while reducing the above described risks associated with each party. In some embodiments, the technique is realized by providing a secured network that stores consumer data in protected environment. In addition, some embodiments of the secured network

---

[1] Our decision will make reference to the Appellants' Appeal Brief ("App. Br.," filed May 4, 2007) and Reply Brief ("Reply Br.," filed Oct. 29, 2007), and the Examiner's Answer ("Answer," mailed Aug. 29, 2007).

may include an approved list of vendors that satisfy predetermined criteria." (Specification 4:6-15).

Claim 1, reproduced below, is illustrative of the subject matter on appeal.

> 1. A method for enabling E-commerce transactions between a vendor and a consumer using a secured network having a host with stored consumer data and approved vendor information, the method comprising the steps of:
>
> enabling the consumer to initiate an E-commerce transaction with the vendor;
>
> enabling the vendor to transmit transaction information related to the E-commerce transaction to the host;
>
> receiving transaction information from the vendor at the host;
>
> processing the transaction information at the host to determine whether the transaction information conforms with the stored consumer data and approved vendor information; and
>
> delivering to the vendor, via the secured network, the stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information wherein receipt of the stored consumer data by the vendor enables the vendor to receive payment for the E- commerce transaction.

THE REJECTIONS

The Examiner relies upon the following as evidence of unpatentability:

Foster	US 6,332,134 B1	Dec. 18, 2001

Segal	US 6,820,804 B2	Nov. 23, 2004
Weber	US 6,178,409 B1	Jan. 23, 2001

The following rejections are before us for review:

1. Claims 1, 3-5, and 7-12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Foster and Segal.
2. Claims 2 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Foster and Weber.

ISSUES

The first issue before us is whether the Appellants have shown that the Examiner erred in rejecting claims 1, 3-5, and 7-12 under 35 U.S.C. § 103(a) as being unpatentable Foster and Segal. This issue turns on whether Foster and Segal describe a "secured network" as claimed.

The second issue before us is whether the Appellants have shown that the Examiner erred in rejecting claims 2 and 6 under 35 U.S.C. § 103(a) as being unpatentable Foster and Weber. This issue turns on whether it would have been obvious to substitute Foster's network with Weber's VPN.

FINDINGS OF FACT

We find that the following enumerated findings of fact (FF) are supported by at least a preponderance of the evidence. *Ethicon, Inc. v. Quigg*, 849 F.2d 1422, 1427 (Fed. Cir. 1988) (explaining the general evidentiary standard for proceedings before the Office).

The scope and content of the prior art

1. Foster relates to a financial transaction system.

2. Foster (col. 8, ll. 19-28) describes a method whereby a cardholder's browser transmits a request to pay a purchase order and this (along with the purchase order) is entered in the card company's system which then tests (a) to determine whether the cardholder is allowed to make the purchase and (b) whether the merchant is allowed to participate in the transaction. Thus Foster describes a method "to determine whether transaction information conforms with stored consumer data and approved vendor information" (claim 1).
3. Foster (col. 8, ll. 47-50) describes a message being sent to the merchant, upon completion of the transaction, which may include a pre-registered shipping address. Thus Foster describes "delivering to the vendor … the stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information" (claim 1).
4. Foster (col. 2, l. 29) describes using its method over the Internet with the use of IDs and passwords (see col. 5, ll. 16-64). Thus Foster describes using a network having a level of security.
5. Segal relates to a system for performing purchase transactions.
6. Segal (col. 1, ll. 14-28) describes the common credit card processing operation whereby a merchant uses a consumer's credit card number to debit the consumer's account. The consumer signs a receipt with the merchant keeping the original signed receipt and the consumer taking a copy, both of which are evidence of proof of purchase.

7. Weber relates to the "secure, electronic payment in exchange for goods and services purchased over a communication network." (col. 1, ll. 7-9).

8. Weber (col. 91, ll. 50-61) describes "[a] virtual, private network between the Gateway and the host processor is established to expedite host communication."

Any differences between the claimed subject matter and the prior art

9. The claimed subject matter differs from the prior art in that it combines elements separately described in the references.

The level of skill in the art

10. Neither the Examiner nor the Appellants has addressed the level of ordinary skill in the pertinent art of E-commerce. We will therefore consider the cited prior art as representative of the level of ordinary skill in the art. *See Okajima v. Bourdeau,* 261 F.3d 1350, 1355 (Fed. Cir. 2001) ("[T]he absence of specific findings on the level of skill in the art does not give rise to reversible error 'where the prior art itself reflects an appropriate level and a need for testimony is not shown'") (Quoting *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 163 (Fed. Cir. 1985)).

Secondary considerations

11. There is no evidence on record of secondary considerations of non-obviousness for our consideration.

PRINCIPLES OF LAW

Obviousness

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). See also *KSR*, 127 S. Ct. at 1734 ("While the sequence of these questions might be reordered in any particular case, the [Graham] factors continue to define the inquiry that controls.") The Court in Graham further noted that evidence of secondary considerations "might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." 383 U.S. at 17-18.

ANALYSIS

Claims 1, 3-5, and 7-12 are rejected under 35 U.S.C. §103(a) as being unpatentable over Foster and Segal.

The Appellants argued claims 1, 3-5, and 7-12 as a group (App. Br. 6 and Reply Br. 2). We select claim 1 as the representative claim for this group, and the remaining claims 3-5 and 7-12 stand or fall with claim 1. 37 C.F.R. § 41.37(c)(1)(vii) (2007).

The Examiner argued that Foster describes the method of claim 1 except that "Foster fails to explicitly disclose … [that the] receipt of the stored consumer data by the vendor enables the vendor to receive payment for the e-commerce transaction." (Answer 4). Accordingly, the Examiner took the position that Foster describes "[a] method for enabling E-commerce transactions between a vendor and a consumer using a secured network having a host with stored consumer data and approved vendor information, the method comprising the steps of [ ] enabling the consumer to initiate an E-commerce transaction with the vendor; enabling the vendor to transmit transaction information related to the E-commerce transaction to the host; receiving transaction information from the vendor at the host; processing the transaction information at the host to determine whether the transaction information conforms with the stored consumer data and approved vendor information; and delivering to the vendor, via the secured network, the stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information" (claim 1).

For the limitation "wherein receipt of the stored consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction" that ends claim 1 that the Examiner found Foster did not describe, the Examiner relied upon Segal, which the Examiner stated "discloses a system/method for performing a purchase transaction in which a consumer provides a merchant with a credit card for payment." (Answer 4). According to the Examiner, "the merchant [in the Segal process] then uses the credit card number to debit the credit card account of the consumer. The consumer signs a receipt evidencing the transaction. The merchant keeps the original signed receipt and gives the consumer a copy of the signed

receipt. The signed receipts are evidence of proof of purchase for both the consumer and the merchant (*see* [ ] Segal, col. 12, lines 14-28)." (Answer 4).

The Examiner concluded that "it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the financial transaction of Foster by including the limitation detailed above as taught by Segal because this would allow an authorized person to act on behalf of the consumer and purchase goods or services." (Answer 4).

The Examiner's characterization of the scope and content of the prior art and the differences between the claimed subject matter and the prior art appear to be correct. (FF 1-6). All the factual inquiries for a determination of obviousness have been addressed (FF 1-6 and 9-11) and the Examiner appears to have provided an apparent reason with logical underpinning for the legal conclusion of obviousness. Accordingly, we find that a prima facie case of obviousness has been established.

The Appellants disagree. The Appellants have made two arguments.

First, according to the Appellants, Foster does not describe a secured network. Thus, according to the Appellants, Foster fails to "disclose or suggest the limitation in claim 1 of 'delivering to the vendor, *via the secured network*, the stored consumer data.'" (App. Br. 7) (emphasis in original). (*See also* Reply Br. 2-3). According to the Appellants (App. Br. 7), Foster's description of its network is not only not secured but teaches away from a secured network. The Appellants pointed to Foster passages at col. 2, ll. 41-43, which states "[m]ultiple user identifiers (Ids) and passwords (which) can be assigned to different people to obtain credit from the same credit card;" col. 2, ll. 2-6, which states "[t]he secure electronic (SET) protocol, while having promise, has been abandoned by key players in

industry. At this point in time, secure socket layer (SSL) is in the fall back position, particularly on the Internet;" and, col. 2, ll. 32-40, which the Appellants contend "discloses the use of Ids and passwords and the minimizing of transmitting data."

This first argument is not persuasive as to error in the rejection. The argument presupposes that the "secured network" that is claimed is somehow different from the network the Appellants have explained Foster describes. That in turn requires a definition for the claim term "secured" such that the claimed network distinguishes from that of Foster. In that regard, the Appellants do not point us to a definition in the Specification, nor do we find one, which would support the argument that the claim term "secured" defines something different from what Foster describes. Since the Specification provides no explicit definition beyond a general indication that the "[s]ecured network [ ] may comprise any type of network capable of conducting secured transaction" (Specification 9:16-18), we will apply its ordinary and customary meaning as understood by those skilled in the art. The ordinary and customary meaning of "secured" is "to make secure, or safe; guard; protect." (*See Webster's New World Dictionary* ¶ (3rd Ed. 1988.)(Entry 1 for "secured."). In that light, we see no difference between the claimed "secured" network and that of Foster. In using IDs and passwords, which are notoriously well known safeguards for protecting networks, Foster's network is "secured" to the extent claimed. We understand that the Appellants are intending to use a network that has greater security than one that depends on passwords and IDs, but that distinction in levels of security is not reflected in the claim. We must give claims their broadest reasonable construction in light of the Specification as

it would be interpreted by one of ordinary skill in the art. We have done so. To read into the claim a level of security that is not claimed would be to impermissibly narrow the scope of the claim.

Finally, regarding Foster's statement that "[t]he secure electronic (SET) protocol, while having promise, has been abandoned by key players in industry" (which is stressed in the Reply Brief, p. 2) and the Appellants' view that this is a teaching away from using a secured network, we disagree. This is not a teaching away from using a secured network. Simply because Foster describes the abandonment of a particular security protocol does not suggest Foster fails to describe providing security; it simply suggests that a particular security protocol has not shown promise. *Cf. In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994) ("A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use.").

Second, the Appellants noted that the Examiner "acknowledges that Foster fails to disclose that 'receipt of the stored consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction'" and that the Examiner relied on Segal to meet that claimed limitation. (App. Br. 8. *See also* Reply Br. 3-5). However, according to the Appellants, Segal fails to show a secured network. "Segal discloses the user transmitting any required data to the vendor and not the use of the 'secured network' for the receipt of stored consumer data" from "a host with stored consumer data and approved vendor information." (App. Br. 8). The Appellants repeated that Foster does not disclose a secured network. (App. Br. 9). As a result, the Appellants concluded that "the proposed combination of Foster and Segal does not disclose or suggest either transactions via a

'secured network' or a host transmitting data by the vendor wherein the "receipt of consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction." (App. Br. 9).

This second argument is not persuasive as to error in the rejection. The argument is essentially a repeat of the first argument but applied against Segal; i.e., Segal fails to describe a "secured" network. However, the Examiner did not apply Segal as evidence that a secured network is disclosed in the prior art. For that, the Examiner presented Foster. As we explained above, the Appellants have not shown that Foster does not describe a secured network of the kind claimed. Accordingly, the cited prior art, as evidenced by Foster, meets the claimed limitation of a "secured network." We do not see, nor have the Appellants shown, anything in Segal which would have led one of ordinary skill in the art away from using the network "secured" in the manner Foster describes. We are satisfied that Foster meets the claimed limitation of a "secured network" and that, given Segal, one of ordinary skill in the art would have been led to modify Foster's method such that "receipt of consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction."

These being the only arguments challenging the prima facie case of obviousness and having been found unpersuasive and there being no secondary considerations of nonobviousness for our consideration, we will sustain the rejection.

We note the Appellants' discussion of the legal standard for determining obviousness. (App. Br. 9-11; Reply Br. 5-6). Although we find that our analysis meets the approach discussed in the Brief, the discussed approach is more rigid than the flexible approach advocated by the Supreme

Court in its decision in *KSR*. For example, the Appellants contend that the "teaching or suggestion to make the claimed combination and the reasonable expectation of success *must both be found in the prior art*." (App. Br. 10 and Reply Br. 5-6) (emphasis added). That is too rigid an approach for determining obviousness. "The obviousness analysis cannot be confined by a formalistic conception of the words teaching, suggestion, and motivation, or by overemphasis on the importance of published articles and the explicit content of issued patents." *KSR* at 1741. A rigid requirement relying on written prior art or patent references would, as the Supreme Court noted, unduly confine the use of the knowledge and creativity within the grasp of an ordinarily skilled artisan. *Id.* at 1742.

Claims 2 and 6 are rejected under 35 U.S.C. §103(a) as being unpatentable over Foster and Weber.

The Appellants argued claims 2 and 6 as a group (App. Br. 11; Reply Br. 7). We select claim 2 as the representative claim for this group, and the remaining claim 6 stands or falls with claim 2. 37 C.F.R. § 41.37(c)(1)(vii) (2007).

Claim 2 further limits the method of claim 1 in "providing a secured network [which] comprises [ ] providing a virtual provate network (VPN) that enables secured communication of the transaction information."

The Examiner conceded that "Foster does not explicitly disclose the use of a VPN." (Answer 5). The Examiner relied on Weber to meet this limitation. According to the Examiner, "Weber discloses a virtual private network between a gateway and a host processor that is established to expedite host communication (*see* [ ], col. 91, lines 50-61)." (Answer 5).

The Examiner concluded by finding that "it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of [F]oster to utilize a virtual private network as VPN is known to provide greater security when performing transaction." (Answer 5).

The Examiner's characterization of the scope and content of the prior art (FF 7 and 8) and the differences between the claimed subject matter and the prior art appear to be correct. All the factual inquiries for a determination of obviousness have been addressed (FF 1-11) and the Examiner appears to have provided an apparent reason with logical underpinning for the legal conclusion of obviousness. Accordingly, we find that a prima facie case of obviousness has been established.

The Appellants argued that, notwithstanding that Weber describes a VPN ("Weber discloses a "virtual, private network [VPN] between the Gateway and the host processor," col. 91, lines 50-51, … ." App. Br. 12), "Weber discloses the use of a VPN only within a corporate gateway to a corporate host." (App. Br. 12; Reply Br. 7). The Appellants contend that "Weber does not disclose or suggest the use of VPNs between a host and a vendor." (App. Br. 12; Reply Br. 8).

We are not persuaded by the Appellants' argument.

The issue is whether it would have been obvious to substitute a VPN for the network in Foster in light of Weber. There is no dispute that VPNs provide a degree of security. We see nothing unpredictable in replacing Foster's network with that of Weber's. The Supreme Court pointed out that "[n]either the enactment of § 103 nor the analysis in *Graham* disturbed this Court's earlier instructions concerning the need for caution in granting a

patent based on the combination of elements found in the prior art." *KSR* at 1739. "In *United States v. Adams,* 383 U.S. 39, 40, 86 S. Ct. 708, 15 L.Ed.2d 572 (1966), a companion case to *Graham,* the Court considered the obviousness of a "wet battery" that varied from prior designs in two ways: It contained water, rather than the acids conventionally employed in storage batteries; and its electrodes were magnesium and cuprous chloride, rather than zinc and silver chloride. The Court recognized that when a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result. 383 U.S., at 50-51, 86 S. Ct. 708." *KSR* at 1739-1740. Here, the Appellants have provided no evidence that substituting Foster's network with a VPN yields anything more that the predictable level of security commonly associated with VPNs.

With regard to the Appellants' point that Weber's use of a VPN is in a corporate rather than a merchant environment, it is not clear to us that this is the case. Given that Weber relates to the "secure, electronic payment in exchange for goods and services purchased over a communication network" (col. 1, ll. 7-9), one of ordinary skill in the art reading Weber would foresee the VPN used in the merchant context involving E-commerce transactions between a consumer and vendor. Nevertheless, we disagree with the implication that one of ordinary skill would not look to corporate business to adapt a merchant business. These areas of business are analogous. One of ordinary skill in the art of E-commerce seeking to make improvements would certainly look to businesses operating in other endeavors for suggestions, and that would include businesses operating in a corporate context. "When a work is available in one field of endeavor, design

incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, § 103 likely bars its patentability." *KSR* at 1740. Again, we see nothing, and the Appellants have not provided evidence to support it, that substituting Foster's network with a VPN yields anything more that the predictable level of security commonly associated with VPNs.

This being the only argument challenging the prima facie case of obviousness and having been found unpersuasive and there being no secondary considerations of nonobviousness for our consideration, we will sustain the rejection.

We note the Appellants' discussion of the legal standard for determining obviousness. (App. Br. 12-14); (Reply Br. 8-10). In response, we incorporate herein our earlier remarks concerning the similar discussion presented at App. Br. 9-11 and Reply Br. 5-6.

CONCLUSIONS OF LAW

We conclude that the Appellants have not shown that the Examiner erred in rejecting claims 1, 3-5, and 7-12 under 35 U.S.C. § 103(a) as being unpatentable over Foster and Segal and claims 2 and 6 under 35 U.S.C. § 103(a) as being unpatentable over Foster and Weber.

DECISION

The decision of the Examiner to reject claims 1-12 is affirmed.

Appeal 2008-3749
Application 09/749,408

AFFIRMED

JRG

James G. Gatto, Esq.
Hunton & Williams
Suite 1200
1900 K Street, N.W.
Washington, DC 20006